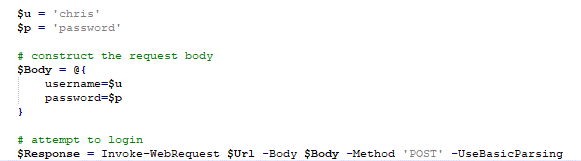
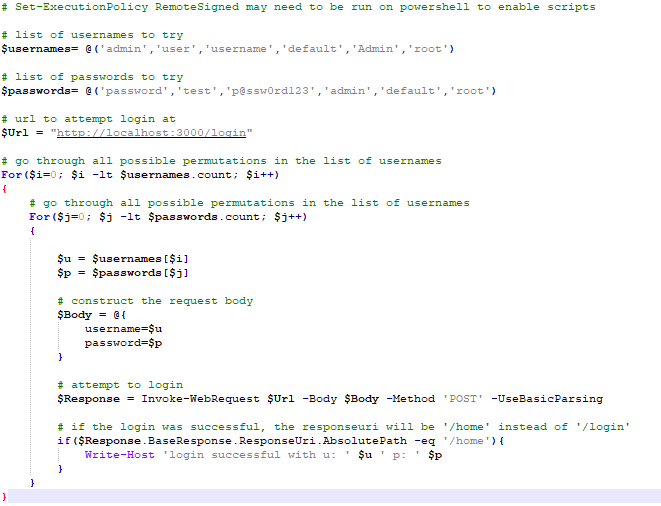
# OWASP 02 – Broken Authentication

## Walkthrough – Shop App

1. Open a terminal/command prompt on your system
2. Create a POST request for the /login page of the application. An example in powershell is below



1. Notice that the web application accepts such requests and returns a response
2. Create a credential stuffing attack by modifying this script to go through a dictionary of usernames and passwords, and attempt login in each pair. An example in powershell is below



1. Notice that some of the combinations worked
2. Log in with those usernames and passwords

## Exercises – Shop App

1. Execute a SQL injection to get a list of usernames from the database
2. Update your script with the list of usernames
3. Update your script with a list of commonly used passwords
4. Update the populatedb.sql script to remove the default administrative credentials
5. Update the shopping application to disallow commonly used passwords on registration – use the list of commonly used passwords you found in problem 3